
45
Anos
CODIGO DE CONDUTA
brt
Consolidadora | Operadora de Turismo

CÓDIGO DE CONDUTA DO GRUPO BRT

ÍNDICE

1. INTRODUÇÃO

O cumprimento das normas internas previstas neste Código é uma obrigação de todos e visa a proteção dos gestores, colaboradores, terceiros, parceiros e da empresa.

Este Código tem a missão de trazer os valores que o GRUPO BRT respeita e assegura na sua atividade empresarial, bem como as regras que irão lhe guiar a respeito do que pode e do que não pode ser realizado no exercício de sua função como colaborador.

A conduta ética empresarial é crítica para nossos negócios. Como empregado, sua responsabilidade é a de compreender, respeitar e aderir a estas práticas, as quais refletem requisitos legais ou regimentais. A violação destas leis e regulamentos podem criar riscos significantes para você, para a empresa, seus diretores, clientes e demais colaboradores da empresa.

Você tem responsabilidade ética em ajudar no cumprimento deste Código e deve estar alerta para possíveis violações e comunicá-las ao tomar conhecimento de quaisquer desvios, utilizando-se dos canais competentes.
A Empresa não permitirá que se façam quaisquer represálias, ameaças, vinganças, retaliações ou ações semelhantes contra qualquer pessoa que denuncie de boa-fé, uma suspeita violação da lei, deste Código ou de outras políticas da Empresa e sempre agirá com base na legislação vigente.

2. VISÃO, MISSÃO E VALORES DO GRUPO BRT

VISÃO

Ser reconhecido pela excelência no atendimento e na prestação de serviços, estar entre os principais players do trade de turismo nacional, além de manter uma relação de confiança e transparência com os nossos clientes.

MISSÃO

Facilitar por meios de recursos tecnológicos, humanos e fornecedores selecionados - acesso a produtos e serviços turísticos, no Brasil e no mundo, para as agências de viagens, oferecendo soluções confiáveis e seguras.

VALORES

Agilidade no atendimento;
Foco na satisfação dos nossos clientes;
Transparência na divulgação e na comercialização de nossos produtos;
Busca contínua da qualidade na prestação de serviços.

3. COLABORADORES: CONDUTAS ACEITAS E CONDUTAS INDESEJÁVEIS

Um ambiente de trabalho de qualidade e respeito aos colegas depende de você e o GRUPO BRT segue esse princípio, priorizando as relações de confiança entre as pessoas, o compromisso com a verdade, resultados e respeito à diversidade, por isso, algumas condutas são aceitas e valorizadas, enquanto outras, são indesejadas e reprovadas, conforme a seguir.

3.1. Preconceitos, assédio moral e sexual

O GRUPO BRT repudia qualquer forma de discriminação, preconceito ou assédios, valorizando a diversidade da nossa equipe de colaboradores, a liberdade de expressão e o respeito às diversas crenças existentes.

3.2. Fraude, suborno e corrupção

O GRUPO BRT não tolera práticas ilícitas dos nossos colaboradores na condução de nossos negócios.

3.3. Saúde, segurança e meio ambiente

O GRUPO BRT tem um compromisso com a saúde do espaço de trabalho, priorizando a segurança de seus colaboradores e o meio ambiente.

3.4. Uso adequado dos bens e recursos

O GRUPO BRT se esforça para fornecer aos colaboradores, os equipamentos e recursos necessários para a realização de suas atividades e para que isto seja possível e sustentável, cabe a todos a obrigação de cuidar e zelar pela preservação do bem fornecido pela Empresa, fazendo uso de forma ética e segura, além de evitar desperdícios e gastos desnecessários seus e dos outros envolvidos no trabalho, respeitando a sustentabilidade e o meio ambiente.

A Empresa poderá solicitar, a qualquer momento, o dispositivo fornecido ao colaborador para inspeção e principalmente se surgir alguma suspeita de risco de vazamento de informações, uso de software pirata, não licenciado ou de uso indevido do mesmo.

Como a empresa é responsável civilmente pelos atos de seus colaboradores e prepostos, ao proceder o monitoramento, preservará o patrimônio e reputação da empresa e de seus colaboradores, sempre respeitando os princípios da razoabilidade e da proporcionalidade.
São adotados procedimentos que envolvem o controle do acesso físico para assegurar a privacidade das comunicações, manutenção de segurança e a proteção dos seus ativos contra roubo, vazamento de dados confidenciais, mau uso dos recursos disponibilizados e destruição de bens da empresa. Entrar na rede da empresa, nas suas instalações ou mesmo de um concorrente e mudar qualquer informação que não esteja autorizado, mesmo com uso de software, estará enquadrado no crime de adulteração de dados em sistema de informações e poderá sofrer as sanções previstas em lei vigente no país.

3.5. Relacionamento com os clientes

Seu trabalho coloca você em contato com muitos clientes ou potenciais clientes, por isso é importante lembrar que você representa a empresa para as pessoas com quem estiver negociando.
O GRUPO BRT espera que todo colaborador atue de tal maneira que possa valorizar os nossos clientes e ajudar a construir um relacionamento baseado em confiança, qualidade, ética e segurança.

3.6. Relacionamento com os parceiros, fornecedores e terceiros

Os mesmos procedimentos indicados no item anterior deverão ser adotados, caso suas atividades sejam executadas junto a fornecedores e terceiros. O GRUPO BRT recomenda que todas as empresas e pessoas com as quais nos relacionamos, sejam informadas sobre a existência deste Código de Conduta.

O QUE NÃO PODE:

1. Estabelecer relações comerciais com empresas clientes que, reconhecidamente, não observem padrões éticos compatíveis com os do Grupo BRT, ou empresas/fornecedores que não estejam devidamente autorizados pelo responsável do setor.

2. Revelar quaisquer informações de caráter confidencial e sigiloso a que tiver acesso e que diga respeito às relações comerciais da empresa com seus clientes.
3. Usar o cargo que ocupa para dispensar tratamento preferencial ou privilegiado a qualquer cliente em desacordo com as políticas da empresa sem expressa concordância da Diretoria da empresa, aceitar benefícios como: prêmios em espécie ou quaisquer vantagens decorrentes do relacionamento comercial da empresa junto aos fornecedores.
4. Gerar prejuízo para a BRT em decorrência de um equívoco provocado pela agência de viagens, sem autorização da diretoria.
5. Indicar agência de viagens para passageiro de forma direta, com o intuito de obter lucro pessoal.
6. Receber ou enviar presentes ou mimos para colegas da empresa, com vista a facilitar ou angariar simpatia para atendimento de suas solicitações de rotina.

3.7. Viagens pela empresa

Os colaboradores que participam de viagens nacionais ou internacionais a trabalho, especialmente nos casos de acompanhamento de *famtours*, feiras e *workshops*, devem seguir todas as recomendações descritas neste documento, representando GRUPO BRT de forma ética e adequada.

3.8. Participação em treinamentos da empresa

Os colaboradores que forem convidados para participar de treinamentos e eventos promovidos pelo GRUPO BRT deverão ter no mínimo 75% de presença anual, considerando que são para o seu desenvolvimento profissional.

3.9. Informações confidenciais

As informações confidenciais do GRUPO BRT são bens valiosos e fazem parte do patrimônio intelectual, além de ser um diferencial no mercado.

Você deve zelar para que as informações confidenciais ou privilegiadas sejam guardadas ou armazenadas de forma segura, nos servidores da empresa e jamais

compartilhe com terceiros não autorizados ou empresas parceiras e concorrentes.
Todo funcionário, agente e contratante tem a responsabilidade de não divulgar informações confidenciais. Esta responsabilidade inclui a proteção, segurança e disposição adequada de informações confidenciais conforme a política interna da empresa.

O QUE PODE: Você pode trocar informações com empresas parceiras apenas em reuniões de negócios, desde que respeite o limite de confidencialidade de dados e que tenha permissão para tal.

O QUE NÃO PODE E ALGUNS CONSELHOS ÚTEIS:

1. Utilizar informações confidenciais para uso próprio ou de terceiros;
2. Deixar expostas no seu local de trabalho, na tela do seu computador, em impressoras ou em salas de reuniões, informações confidenciais ou privilegiadas da empresa;
3. Apagar ou destruir informações produzidas no exercício da sua função, uma vez que os dados produzidos pelo colaborador na condução do negócio são de propriedade do GRUPO BRT;
4. Discutir, presencialmente ou por telefone, assuntos que envolvam informações confidenciais ou privilegiadas relativas a produtos ou negócios quando estiver em local público como, elevadores, restaurantes, aeroportos, aviões, bem como em ambientes virtuais como salas de bate-papo, blogs ou redes sociais;
5. Em hipótese alguma, trocar informações confidenciais ou privilegiadas com empresas concorrentes;
6. Não fale de assuntos da empresa em ambientes nos quais não se pode garantir a confidencialidade;
7. Ao falar ao telefone, tenha a certeza de que você identificou corretamente seu interlocutor, e trate apenas dos pontos necessários para o exercício de sua função;
8. Os documentos em papel, que contêm informações confidenciais, devem ser guardados em local adequado, como armários ou gavetas, fechados

com chave. Não deixe material confidencial sobre a mesa quando não estão sendo utilizados;

9. Ao terminar uma reunião, apague ou retire o que foi escrito em quadros ou folhas de *flip chart*, destrua os papéis de rascunho utilizados e não continue o assunto nos corredores;
10. O acesso a informações da empresa somente será permitido com a supervisão de um gestor responsável e com a finalidade de atender aos interesses do GRUPO BRT;
11. Caso esteja utilizando equipamentos da empresa, sempre faça backup dos arquivos no servidor da mesma e se precisar orientação, procure o responsável pela TI;
12. É proibido armazenar arquivos nos equipamentos corporativos, que não sejam de assuntos do GRUPO BRT;
13. O descarte de disco rígido (HD) é especialmente perigoso, por isso sempre deve ser feito sob a supervisão do responsável de TI;
14. O mesmo é válido para equipamentos descartados ou doados a terceiros;
15. Documentos e dados de cartões de créditos de clientes não poderão ser enviados através de equipamentos pessoais de forma alguma e o vazamento destes dados sensíveis poderá dar razão a ações judiciais nas esferas trabalhista, cível e criminal;
16. Também é proibido encaminhar mensagens eletrônicas de informações confidenciais ou privilegiadas para o seu *e-mail* pessoal ou documentos de clientes para ou de seu dispositivo eletrônico pessoal.
17. Revelar dados e solicitações de um cliente para outro.
18. **Os dados de pagamento de bilhetes emitidos no GRUPO BRT são sigilosos, serão tratados de acordo com a Norma PCI-DSS, disponibilizada no diretório Política de Segurança da Informação.**

3.10. Segurança da informação

Você precisa saber que todos os dados produzidos em razão da atividade profissional, criados, recebidos ou armazenados em computador, *e-mail*, celular corporativo, na rede ou nos sistemas informatizados são de propriedade do GRUPO BRT.

Garantir a segurança desse patrimônio é uma preocupação do GRUPO BRT, pois uma vez divulgado de forma equivocada ou indevidamente, pode gerar prejuízos incalculáveis à empresa e aos nossos clientes.

O QUE PODE: Você pode se deslocar do seu lugar de trabalho, mas não sem antes bloquear ou desconectar seu computador, evitando a utilização por outras pessoas que não você. Lembre-se: a senha de acesso é sua assinatura digital e o seu compartilhamento configura ato ilícito e quem fizer uso de sua senha estará praticando o crime de falsa identidade.

O QUE NÃO PODE:

1. Instalar softwares sem licença apropriada e sem a permissão da T.I, sendo que as licenças necessariamente têm que ser na versão profissional;
2. Compartilhar, em hipótese alguma, suas credenciais, sejam elas *login*, senha ou crachá. Esses dados são individuais e intransferíveis e sua guarda, sigilo e manutenção são de responsabilidade do colaborador ou, prestador de serviços;
3. Utilizar da senha de outro colaborador para realizar qualquer atividade, mesmo que tenha ordem expressa do titular para tal;
4. Compartilhar o acesso da sua caixa individual de *e-mail* a outro colaborador ou terceiro;
5. Não utilize senha curta, o ideal é ela tenha pelo menos oito ou mais caracteres, inclusive que tenha caracteres especiais como $ # @ e letras maiúsculas/minúsculas;
6. Sempre misture letras, números e símbolos. Quanto mais diversificada for uma senha, mais segura ela será;
7. Jamais repita sua identificação (login) como senha;
8. Ao receber a senha padrão modifique-a logo a seguir, você é o único responsável por sua senha e sua garantia de maior segurança;
9. Adote uma senha fácil de ser lembrada por você e difícil de ser identificada por outra pessoa;
10. Mude a senha pelo menos uma vez a cada seis meses;
11. Nunca anote a senha em lugar visível, sempre procure memorizar;

12. Importante lembrar que usar senha de outro é crime tipificado no ordenamento jurídico: ***Art. 307 CP: crime de "falsa identidade": Pena - Detenção, de 3 (três) meses a 1 (um) ano, ou multa, se o fato não constitui elemento de crime mais grave.*** Saiba também que é crime tipificado no Art. 154-A da Lei 12.737/2003, "*Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".*

3.11. Uso dos meios eletrônicos

O GRUPO BRT é favor da utilização de todos os recursos eletrônicos disponíveis, desde **que direcionados para o exercício da atividade profissional que você desempenha e estejam autorizados pela empresa**. Esta regra é muito importante para que possamos cumprir nossas metas e preservar nossos empregos e atender de forma ética e segura nossos clientes e parceiros comerciais.

De acordo com o Código Civil, o GRUPO BRT é responsável pelos atos de seus colaboradores e prestadores e deve, a seu critério, **usar e monitorar quaisquer informações transacionadas no ambiente corporativo**.

Essa norma abrange todas as informações transacionadas pelos seus colaboradores, parceiros e terceiros, que fizerem uso dos recursos tecnológicos do Grupo BRT, ou mesmo dos seus recursos pessoais, durante o seu horário de trabalho. Desta forma, o seu *e-mail* corporativo, recursos utilizados para mensagens eletrônicas e qualquer equipamento ou sistema pessoal usado em equipamentos ou na rede da organização, poderá ser monitorado, sem que isso represente qualquer violação de privacidade, posto o caráter profissional de tal utilização, inclusive estabelecendo tratamento igual para todos os colaboradores, gestores e terceiros.

Os recursos de comunicação autorizados para atender nossos clientes e parceiros do Grupo BRT são:

- *E-mail* corporativo (ex.: colaborador@grupobrt.com.br)
- *Telefone fixo*
- *Google Hangouts*: para a comunicação com os clientes via texto e vídeo
- Telefone móvel corporativo: para os que tiverem autorização
- Notebook corporativo: para os que tiverem autorização

A utilização de software deverá ser autorizada pela área de TI, sendo terminantemente proibido o uso de software pirata ou não licenciado, o descumprimento desta regra poderá resultar em demanda judicial ou cível contra quem gerar prejuízos financeiros ao GRUPO BRT.
Qualquer dúvida sobre a instalação ou uso destes recursos poderá ser esclarecido pelo responsável da TI. O *Skype*, telefone pessoal, outras redes sociais e demais recursos não apontados nos itens acima, não estão autorizados para uso no desempenho de suas atribuições como colaborador ou prestador de serviço para o Grupo BRT, salvo departamentos que necessitam de recursos específicos e com autorização dos gestores.
Não é permitido o uso de serviços de *streaming*, tais como rádios e TV's online, exceto para o recebimento de informações pertinentes ao exercício de suas funções.

3.11.1. *Internet*

Trata-se de um ambiente não seguro, mas necessário em alguns momentos da nossa prestação de serviços e para minimizar os riscos são necessários alguns cuidados básicos:

1. Nunca instale programas disponíveis na Internet, sem antes consultar a área de TI;
2. Não acesse sites desconhecidos ou de conteúdo duvidoso;
3. Nunca acesse sites indicados em *e-mails*, sem antes consultar a pessoa que enviou para estar certo de que não causará nenhum dano a você ou a empresa;

4. Material sexualmente explícito não pode ser acessado, exposto, armazenado, distribuído, editado, impresso ou gravado;
5. É totalmente proibida a divulgação ou acesso a conteúdo pedófilo;
6. A utilização de qualquer recurso da empresa para atividades ilícitas será punida, com penas previstas pela empresa e nas leis vigentes, sendo obrigação de todos colaborar com as autoridades policiais na apuração de eventuais crimes;
7. Ninguém pode utilizar recursos tecnológicos da empresa para fazer *download* ou distribuição de software, músicas, vídeos ou dados pirateados;
8. Sendo do interesse da empresa que seus colaboradores estejam sempre bem informados, o acesso a sites de notícias é permitido, desde que com moderação para não comprometer suas tarefas diárias e tão pouco a banda de *internet*;
9. Importante que todos lembrem que o anonimato é vedado em nossa Constituição no artigo 5 (inciso IV – "é livre a manifestação do pensamento, sendo vedado o anonimato");
10. Nunca revele informações pessoais, dos clientes ou da empresa neste ambiente;
11. Mantenha seu navegador sempre atualizado, caso não saiba como fazer, peça auxílio ao responsável de TI;
12. A internet corporativa é para uso exclusivo do trabalho, sendo proibido baixar, ouvir, acessar e pesquisar músicas, filmes, jogos e utilizar comunicadores instantâneos para tratar de assuntos pessoais durante o expediente;
13. A empresa poderá penalizar o colaborador ou parceiro que não preserve a imagem do Grupo BRT na internet. A postura de cada um nas redes sociais, internet e mensagens nos comunicadores instantâneos, deverá ser pautada na ética e respeito à sua imagem, de seus parceiros, clientes e de sua empresa.

3.11.2. *E-mail*

Para o uso adequado do *e-mail*, é necessário adotar alguns cuidados:

1. Antes de enviar uma mensagem para um destinatário, veja se realmente precisa enviar cópia para outras pessoas;
2. Certifique-se que o endereço de destino esteja correto, caso aconteça de enviar para a pessoa errada, encaminhe novo *e-mail* pedindo desculpas, solicitando para desconsiderar a mensagem. Use sempre um texto em sua assinatura, informando esse procedimento. ex. "caso você não seja destinatário deste *e-mail*, peço por favor que o desconsidere e apague";
3. Nunca forneça seu *e-mail* a estranhos, somente para as pessoas que realmente possam se interessar pelos serviços da empresa;
4. Ao enviar um *e-mail* para vários destinatários, não revele a lista dos endereços para todos (utilize o campo “CCO” – “cópia carbono oculta”);
5. Desconfie sempre de mensagens enviadas por remetentes desconhecidos e nunca abra ou execute o arquivo anexo, se estiver em dúvida, entre em contato com o pessoal de TI;
6. Caso receba alguma ameaça de sequestro de dados (*ransomware*), por favor não responda ao *e-mail*, não clique em nenhum arquivo e avise imediatamente seu responsável na empresa do ocorrido;
7. Não responda, não abra e nem execute anexos vindos em spams.

3.11.3. Ambiente de rede local via cabo e *wi-fi*

1. Os computadores utilizados como estações de trabalho estão invariavelmente conectados a uma rede local via cabo ou via *wi-fi*, de forma a compartilhar recursos e informações;
2. As definições de acesso a pastas de uso compartilhado no servidor de arquivos devem ser validadas rotineiramente, de forma a não haver quebra de segurança devido a transferências ocasionais de colaboradores entre departamentos, novas contratações ou afastamentos;
3. O GRUPO BRT também faz sua parte para cuidar das informações. Os dados armazenados na rede corporativa são de propriedade da companhia e seu acesso deve ser autorizado, assim sendo, todas as ações realizadas dentro da rede corporativa podem ser monitoradas e registradas a qualquer momento, mesmo sem aviso prévio;

4. Os acessos à rede local seguem o mesmo horário de trabalho registrado para cada colaborador, qualquer necessidade em acessar em horário diferente, o gestor responsável deverá autorizar previamente;

O acesso via *wi-fi também* será feito via *login* e senha nas dependências do GRUPO BRT, somente para pessoas autorizadas.

Caso o visitante precise ter acesso à internet, deverá solicitar a senha para o colaborador da empresa que estiver visitando, sendo que essa senha é válida por 6 horas. Esta senha não poderá ser utilizada pelos colaboradores do Grupo BRT, com exceção dos que estiverem em salas de reuniões e que estejam portando notebook da empresa.

Responder *e-mail*s, mensagens eletrônicas, atender ou fazer ligações fora do seu horário de trabalho será por liberalidade de cada um. A empresa não exigirá que você desempenhe sua atividade profissional fora dos dias e horários pré-definidos como sendo sua jornada de trabalho. O acesso a VPN fora do expediente normal segue a mesma regra.

3.11.4. Cópias de segurança

O armazenamento de arquivos eletrônicos deverá ser feito sempre no servidor de arquivos, onde existe um procedimento sistemático de cópia de segurança centralizada e regular (*backup*). Caso não conheça os procedimentos, solicite ajuda ao pessoal de TI.

1. Você deve fazer cópias diárias de segurança dos arquivos que estejam armazenados em seu computador no servidor da empresa;
2. Lembre-se que os *pendrives* são dispositivos para transporte e não para armazenamento de dados de forma contínua;
3. Faça sempre backup de seus arquivos no servidor da empresa (*Google Drive*) e nunca nos dispositivos móveis;
4. Caso faça uso de notebook da empresa, os backups deverão ser feitos todos os dias e, por motivo de segurança, os arquivos pertencentes à empresa não deverão ser mantidos no equipamento móvel.

3.11.5. Proteção de dispositivos móveis

O roubo de dispositivos móveis, como *notebooks*, *tablets*, *e smartphones*, é cada vez mais comum hoje em dia.

Para minimizar os riscos com o seu equipamento, sugerimos os seguintes procedimentos descritos a seguir:

1. Todos os equipamentos portáteis que permanecem nas instalações da empresa devem ser guardados em local seguro, devidamente protegido;
2. Ao transportar o seu *notebook* no carro, coloque-o sempre no porta-malas para que não fique visível e esteja mais protegido. Evite deixá-lo no veículo quando estiver estacionado. Lembre-se que você também é responsável pela quebra ou extravio do mesmo;
3. Uma ferramenta que auxilia a proteção da informação de notebooks, discos rígidos portáteis e *pendrives* é a criptografia de dados. Consulte a área de TI;
4. É de responsabilidade do usuário assegurar a integridade de seu equipamento e a confidencialidade das informações nele contidas. Em caso de roubo ou perda comunique imediatamente a sua chefia e a área de TI, que adotará as orientações previstas na Política de Segurança da Informação;
5. Mantenha sempre todos os dispositivos móveis com senha, l*ogin e softwares licenciados e atualizados*;
6. Caso seja autorizado a utilizar um equipamento móvel particular, o colaborador terá que assinar "Termo de Uso de Dispositivo Móvel Pessoal" em anexo e seguir todas as orientações constantes do mesmo;
7. Lembrando novamente que todos os arquivos da empresa devem ser salvos no servidor e nunca devem permanecer no equipamento móvel e tanto o equipamento como os dados são de responsabilidade do usuário.

3.12. Responsabilidades e sanções

Colaboradores

Todos os colaboradores são responsáveis pela segurança das informações empresariais, independentemente de seu nível hierárquico, inclusive em ajudar

a divulgar a cultura de segurança da informação na empresa e fiscalizar para ver se todos estão cumprindo.

Gestores
São os responsáveis pela instrução de seus colaboradores diretos sobre os riscos e os fatores críticos de segurança dentro do âmbito de seus próprios departamentos, considerando as particularidades existentes.

Sanções
O descumprimento das regras de uso da Internet, dos recursos de tecnologia e demais normas de conduta descritas neste documento e na Política de Segurança da Informação, acarretará sanções, como:

- Na primeira vez o colaborador receberá advertência verbal e/ou por escrito;
- Na segunda, poderá ter seu descumprimento registrado em sua ficha de trabalho;
- E na terceira e última advertência, será dispensado por Justa Causa - Conforme previsto na Consolidação das Leis Trabalhistas - CLT, com base nos seguintes dispositivos:

  Art. 482 - Constituem justa causa para rescisão do contrato de trabalho pelo empregador:
  a) ato de improbidade;
  b) incontinência de conduta ou mau procedimento;
  e) desídia no desempenho das respectivas funções;
  g) violação de segredo da empresa;
  h) ato de indisciplina ou de insubordinação;

4. GERENCIAMENTO DAS CONDUTAS NO GRUPO BRT

4.1. Sempre que você identificar descumprimento deste Código por alguém, deve reportar à área de Recursos Humanos.

4.2. A empresa poderá aplicar sanções disciplinares permitidas em lei, para coibir ações que violem estas ou quaisquer outras políticas da Empresa, que podem incluir advertência ou suspensão, desligamento sem justa causa ou por justa causa, até mesmo a responsabilização cível e criminal dos envolvidos.
4.3. Nos casos de violação das leis em vigência no país, a empresa irá cooperar com as autoridades competentes no fornecimento de todos os elementos que visem elucidar a verdade dos fatos e responsabilização dos infratores.
4.4. Exceções ou situações não previstas neste Código ou em nosso ordenamento jurídico, serão tratadas caso a caso pela Diretoria.
4.5. **Esses compromissos permanecem válidos mesmo após o encerramento do seu contrato de trabalho com o GRUPO BRT.**

5. DOCUMENTOS COMPLEMENTARES PARA CONSULTA

Documentos internos

- Política de Segurança da Informação
- Termo de responsabilidade de inclusão em grupos de WhatsApp durante o horário de trabalho
- Termo de concessão e uso de aparelho de telefonia celular
- Termo de concessão e uso de aparelho de computador portátil
- Norma de uso de dispositivos móveis pessoais - BYOD
- Termo de sigilo e confidencialidade (CLT)
- Termo aditivo de contrato de trabalho (danos e prejuízos - CLT)
- Declaração de conflito de interesses (CLT)
- Acordo de cessão de direito de uso de nome e imagem (CLT)

Bibliografia

Beal, Adriana. *Segurança da Informação*, São Paulo: Atlas, 2005.
Ferreira, Fernando e Araújo, Márcio. *Política de Segurança da Informação– Guia Prático de Elaboração e Implementação*, São Paulo: Ciência Moderna, 2006.
Fontes, Edilson Luiz Gonçalves. *Segurança da Informação – O usuário faz a diferença*, São Paulo: Saraiva, 2006.
NBR ISO/IEC 27001:2006 – *Técnicas de gestão da segurança da informação*.

OGC. *ITIL Best Practice on Security Management*, London: Stationary Office, 2005.
Lei nº 12.846/14 – Lei Anticorrupção.
Lei 12.737/14 - Lei dos Crimes Eletrônicos.
Lei 12.965/14 Marco Civil da Internet.
Lei de Provas nº 12.850/2013.
Decreto n.º 7.845/12 que regulamenta procedimentos de segurança e tratamento da informação classificada.
Gonçalves, Victor Hugo Pereira. *Marco Civil da Internet Comentado*. 1. Ed. - São Paulo: Atlas, 2.017.

6. *GLOSSÁRIO*

Antivírus: *Sistema de proteção contra vírus de computador e outras pragas digitais.*
Anti-spam: *Sistema para bloquear mensagens classificadas como spam.*
Backup: *Cópia de segurança.*
E-mail: *Mensagem eletrônica, o mesmo que correio eletrônico.*
HD: *Dispositivo de armazenamento.*
Hacker: Os hackers têm como prática a quebra da segurança de um software e usam seu conhecimento de forma ilegal e são vistos como criminosos.
Wi-fi: *Wireless Fidelity* ***-*** *significa fidelidade sem fio*
Cracker*:* Utilizam todo o seu conhecimento para melhorar softwares de forma legal e nunca invadem um sistema com o intuito de causar danos.
Login*: Conjunto de caracteres solicitado para os usuários que por algum motivo necessitam acessar algum sistema computacional;*
Link: *Terminologia para endereço na internet;*
Malware: *Nome genérico das pragas digitais.*
Mídia: *Qualquer dispositivo de armazenamento, seja magnético (pendrives, HDs) ou ótico (CDs, DVDs).*
Outlook: *Programa da Microsoft para ler e enviar e-mails.*
Pendrive: *Dispositivo para armazenamento de dados temporário, utilizado para transporte, muito usado pelo baixo custo e praticidade.*

Ransomware: *Código malicioso que torna inacessíveis os dados armazenados e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário. O pagamento do resgate geralmente é feito via bitcoins.*
***Servidor**: Computador de maior porte que fornece serviços a uma rede de computadores, como armazenamento de arquivos, impressão, e-mail e outros.*
***Spam**: Mensagem não-solicitada enviada em massa.*
***Spyware:** Programas que violem a privacidade de usuários, transmitindo informações pessoais a terceiros.*
***Stalking:** Constrangimento ilegal que significa a perseguição de uma pessoa por outra. Na internet é comum encontrarmos pessoas que agem pela obsessão na observação de comportamentos em redes sociais ou realização de ameaças, dentre outras condutas;*
***Trojan:** Praga digital que invade computadores escondido em outros sistemas.*
***Vírus**: Programa auto replicável criado com o intuito de causar danos aos sistemas de informação.*
***VPN**:*
***Whatsapp:** Sistemas de mensagens de propriedade do Facebook.*
***Webmail:** Sistema que permite ler e enviar e-mails pelo navegador de Internet.*

7. PRINCIPAIS DELITOS COMETIDOS NO MUNDO REAL E VIRTUAL

Nossas leis aplicam-se ao uso da internet porque tratam de condutas e não de meios. Em especial o artigo 482 da CLT, trata a violação de sigilo ou segredo como delito sujeito a demissão por justa causa para rescisão do contrato de trabalho pelo empregador – "violação de segredo de empresa".

Neste mesmo sentido, a **Lei de Crimes Eletrônicos**, conhecido como "lei Carolina Dieckmann", estabelece que é proibido violar código de segurança (senha) do equipamento de outrem para tirar algum proveito. Outros crimes comuns e que são previstos em nosso ordenamento jurídico:

- Enviar *e-mail* para terceiros com informação considerada confidencial. Divulgação de segredo – art.153 do CP;

- Se manifestar em redes sociais de forma racista ou acusatória (ex.: “chamar de ladrão”). Calúnia – art. 138 do código penal – CP e preconceito de discriminação raça-cor-etnia – art. 20 da lei 7.716/89;
- Enviar vírus que destrua equipamento ou conteúdo. Dano – art. 163 do CP;
- Encaminhar boatos para diversas pessoas. Difamação – art. 139 – CP
- Usar cópia de software sem ter licença- violação ao direito autoral – art. 184.CP
- Usar logomarca de empresa sem autorização do titular. Crime contra a propriedade industrial – art. 195 da lei 9.279/96
- Criar comunidade para ensinar seguidores como fazer algo ilícito. Incitação ao crime – art. 286 do CP
- Participar do Cassino Online – Jogo de azar – art. 180 da CF;
- Ver ou compartilhar fotos de crianças nuas online – Pedofilia – art. “Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente”;
- Enviar *e-mail* com remetente falso, ou mesmo fazer uso de senha de terceiro – Crime de falsa identidade - art. 307 do CP.

Importante lembrar que o desconhecimento da Lei é inescusável, ou seja, todos devem saber o que é proibido, tanto no mundo real, quanto virtual.

8. TERMO DE COMPROVAÇÃO DO RECEBIMENTO DO CÓDIGO DE CONDUTA

Declaro que recebi, li, tomei ciência dos padrões de conduta contidos no Código de Conduta do GRUPO BRT, que não fiquei em dúvida sobre as recomendações apresentadas e entendi que além do aqui disposto podem haver políticas ou normas e procedimentos específicos adicionais para o exercício de minhas atividades na empresa. Compreendi, também, que se surgirem outras dúvidas relativas ao significado ou aplicação deste Código e devo consultar imediatamente o meu superior ou a diretoria. Dessa forma, diante de minha identificação e assinaturas abaixo, declaro que estou ciente do conteúdo e da importância em seguir o disposto neste documento, e que concordo, expressamente, em cumpri-lo em sua íntegra.

Local e data:
Nome:
Documento de Identidade:

Assinatura:

Versão atualizada em 08/2018